QUESTION ONE

Confidentiality, Integrity, and Availability Requirements for Automated Cash Deposit Machines

Confidentiality: Protecting user financial and personal data, such as balance and account numbers, from unauthorized access or disclosure is paramount. Ensuring encrypted and secure communication between the machine and the banking system is crucial to prevent eavesdropping and identity theft. Confidentiality is vital for maintaining system credibility and user trust, preventing financial fraud.

Integrity: Accurate and reliable processing of transactions is essential. Ensuring that user account balances are correctly updated and that cash deposit procedures are precise and thorough prevents unauthorized modifications and tampering with transaction data. Integrity safeguards the system's reliability and credibility.

Availability: Ensuring continuous user access to the cash deposit machine is important, though short-term disruptions may be tolerated if alternative deposit methods are provided. High availability ensures a seamless user experience, though it is secondary to confidentiality and integrity.

Significance: While all three aspects are important, confidentiality and integrity are critical for maintaining user trust and preventing fraud, whereas availability, though necessary, can be mitigated with alternative solutions.

QUESTION TWO

Evaluating Confidentiality, Integrity, and Availability in Various Contexts

1. Student Blog (Public Information)

Confidentiality: Low. Since the blog is a public resource, secrecy is not a priority.

Availability: Low. Outages are inconvenient but have no **serious** consequences.

Integrity: Moderate. Ensuring the information published is accurate and reliable.

2. University Examination Section (Sensitive Exam Information)

Confidentiality: High. Public disclosure of exam papers could jeopardize the examination process.

-Availability: High. Necessary for exam preparation, administration, and grading.

Integrity: High. Essential for maintaining the accuracy and reliability of exam content.

3. Pathological Laboratory Information System (Patient Data)

Confidentiality: High. Breaches could lead to severe privacy violations.

Availability: High. Timely and accurate diagnoses and treatments depend on system availability.

Integrity: High. Accurate medical records and treatment plans are critical.

4. University Student Information System (Personal and Academic Data)

Confidentiality: High. Protects sensitive personal and academic data.

Availability: Moderate. Important for administrative processes but not critical.

Integrity: High. Ensures correct academic records and personal data.

5. University Library Management System (Student and Book Data)

Confidentiality: Moderate. Student data is sensitive but not critical.

Availability: Moderate. Important for library operations but not critical.

Integrity: Moderate. Ensures accurate records of student borrowing and book inventory.

Overall Evaluation: Each system requires a tailored approach to confidentiality, integrity, and availability based on the sensitivity and criticality of the information they handle.

QUESTION THREE

Overview of Data Protection Regulations and Standards

Data Protection Act:

Aimed at safeguarding confidential information stored digitally or in organized paper files, the Data Protection Act imposes obligations on data managers and processors, providing individuals with rights over their data. Key provisions include:

Rights of Individuals: Access to personal data, error correction, and deletion requests.

Data Processing Principles: Lawful, fair, and transparent processing; purpose limitation; data minimization; accuracy; storage limitation; and security.

Accountability and Governance: Establishing data protection officers and conducting impact assessments to ensure compliance.

General Data Protection Regulation (GDPR):

Supplementing the Data Protection Act in the UK, GDPR sets stringent guidelines for data protection and privacy.

ISO 27001:

A global standard for information security management systems (ISMS), ISO 27001 provides a systematic approach to managing sensitive company data. Key elements include:

Risk Management: Densifying and mitigating information security risks.

SMS Framework: Implementing policies and controls for data security.

Continuous Improvement: Regular reviews and updates to maintain ISMS effectiveness.

Annex A Controls: Security measures covering physical security, incident handling, cryptographic controls, and access control.

National Institute of Standards and Technology (NIST):

A U.S. federal agency, NIST advances measurement standards in technology and cybersecurity. Key contributions include:

Cybersecurity Framework: Best practices for enhancing cybersecurity risk management.

Special Publications: Guidelines for information security, including NIST SP 800-171 and SP 800-53.

Standards Development: Collaborating with stakeholders to ensure technology security and interoperability.

Implementing these standards and regulations helps organizations protect sensitive data, enhance trust, and meet legal obligations.